(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－254897

(43)公開日　平成７年(1995)10月３日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
Ｇ０９Ｃ	1/00		9364－5L		
				Ｈ０４Ｌ　9/ 00　Ｚ	

審査請求　未請求　請求項の数19　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願平6－88526

(22)出願日　平成６年(1994)４月26日

(31)優先権主張番号　０８／０５６５４７

(32)優先日　1993年５月５日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　594071860
アディソン・エム・フィッシャー
アメリカ合衆国　フロリダ州33942，ネイプルズ，マーチャンタイル・アベニュー，4073番

(72)発明者　アディソン・エム・フィッシャー
アメリカ合衆国　フロリダ州33942，ネイプルズ，マーチャンタイル・アベニュー，4073番

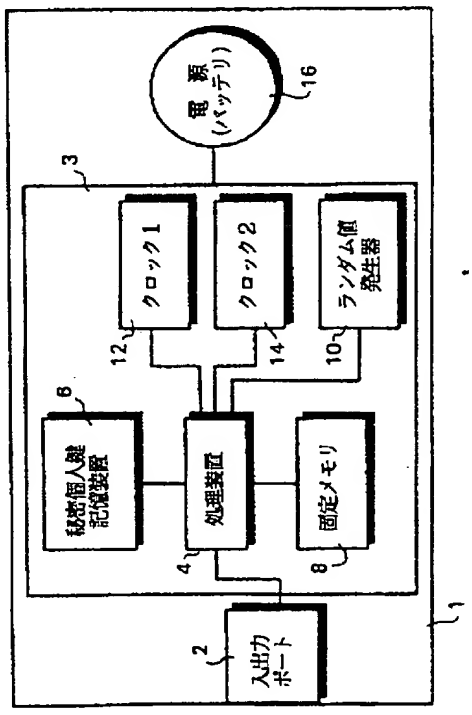
(74)代理人　弁理士　小笠原　史朗

(54)【発明の名称】　個人用日時認証装置

(57)【要約】　（修正有）

【目的】　時刻認証を署名操作と組合わせ、タイムスタンプ装置を不必要にする。

【構成】　携帯用認証装置１は入出力ポート２を含み、入出力ポート２は単一の集積回路チップ３に結合する。入出力ポート２は、交互にＰＣまたはラップトップコンピュータなどに結合される従来のスマートカード読取装置に結合してもよい。変更防止の秘密個人鍵記憶装置６がチップ３上に設けられる。個人鍵記憶装置６は処理装置４と結合され、相互に処理装置４によって実行されるプログラムを記憶する固定メモリ８と結合される。少なくとも１つのクロックがカード上に設けられる。第２のクロック１４およびランダム値発生器１０も処理装置４に結合される。装置１はデジタル時間認証をデジタル署名操作に組み合わせ、タイムスタンプが常に自動的に提供されることを保証する。



1

【特許請求の範囲】

【請求項１】　ユーザが携行する携帯用媒体上に作成されるトークン装置であって、

前記ユーザに関連するデジタル署名を行うために用いられる機密性を有する個人鍵を少なくとも１つ記憶する記憶装置と、

日時表示を提供するためのクロックと、

デジタル的に署名されるべき値を受信し、出力するための通信ポートと、

前記通信ポートおよび前記クロックと結合され、デジタル的に署名されるべき前記値および前記日時表示を受信し、前記通信ポートに出力するために前記少なくとも１つの個人鍵で少なくとも１つのデジタル署名を行うための処理装置とを備える、トークン装置。

【請求項２】　前記処理装置に結合されたランダム数発生器をさらに備える、請求項１に記載のトークン装置。

【請求項３】　前記処理装置に結合された追加のクロックをさらに含む、請求項１に記載のトークン装置。

【請求項４】　前記処理装置は、ユーザの個人識別パスワード（ＰＩＮ）を、デジタル署名を提供するために必須なものとして確認するための手段を含む、請求項１に記載のトークン装置。

【請求項５】　前記処理装置は、改変する試みに応答してデジタル署名ができないようになる、請求項１に記載のトークン装置。

【請求項６】　前記機密性を有する記憶装置は複数の個人鍵を記憶し、前記処理装置は前記複数の個人鍵を用いて少なくとも１つのデジタル署名操作を行う、請求項１に記載のトークン装置。

【請求項７】　ユーザトークン装置を操作する方法であって、

ａ）デジタル的に署名されるべきデジタル値を受信するステップと、

ｂ）信頼性のあるクロック源から現在時刻を決定するステップと、

ｃ）現在時刻と、署名されるべき情報から抽出された値とを含むデジタルデータ構造を作成するステップと、

ｄ）少なくとも１つの記憶された個人鍵にアクセスするステップと、

ｅ）デジタルデータの前記構造にデジタル的に署名するステップとを備える、操作方法。

【請求項８】　前記少なくとも１つの記憶された個人鍵は、機密性を有する時間認証装置内から操作する個人鍵を有することが証明されている関連する公開鍵を有する、請求項７に記載の操作方法。

【請求項９】　前記少なくとも１つの個人鍵は、特定の個人を識別することが証明されている関連する公開鍵を有する、請求項７に記載の操作方法。

【請求項１０】　前記少なくとも１つの記憶された個人鍵と関連する少なくとも１つの証書が、装置内に記憶されている、請求項７に記載の操作方法。

2

【請求項１１】　前記少なくとも１つの記憶された個人鍵と関連する証書の内の１つは、装置外に記憶されている、請求項７に記載の操作方法。

【請求項１２】　前記クロックは、製造時に恒久的な初期設定が行われる、請求項７に記載の操作方法。

【請求項１３】　前記個人鍵の内の少なくとも１つは、製造時に作成される、請求項７に記載の操作方法。

【請求項１４】　ユーザトークン装置を基礎にしたシステムであって、

前記ユーザに関連するデジタル署名を行うために用いられる機密性を有する個人鍵を少なくとも１つ記憶する記憶手段と、

入力デジタル信号を受信し、デジタル出力を発信するための通信手段と、

前記入力デジタル信号を受信し、前記の少なくとも１つの個人鍵でデジタル署名を行うための処理手段と、

信頼性のある日時認証装置とインタフェイスし、前記通信手段を通って前記認証装置によって作成された日時に関する信号と前記処理手段とを結合するための手段とを備える、ユーザトークン装置システム。

【請求項１５】　前記機密性を有する記憶手段は、信頼性のある日時認証装置を識別するために用いられる情報を記憶する、請求項１４に記載のシステム。

【請求項１６】　前記インタフェイス手段は、少なくとも１つの信頼性のある時刻認証装置と結合されたトークン装置に入出力を供給するために、使用時に、少なくとも１つのインタフェイス読取装置と結合される、請求項１４に記載のシステム。

【請求項１７】　個々の偏差を補償してオンチップクロック装置を較正するための方法であって、

マスタクロックから第１のクロック読み取りを行うステップと、

第１のクロック読み取りを記憶するステップと、

マスタクロックから第２のクロック読み取りを行うステップと、

第２のクロック読み取りを記憶するステップと、

両方のマスタクロック読み取りの振動数をカウントするステップと、

第２および第１のマスタクロック読み取りの差を用いて単位時間当たりの振動を計算し、実際の振動数を決定するステップと、

計算された振動数を記憶するステップと、

オンチップクロック装置の出力を前記計算された振動数に従って調整するステップとを含む、較正方法。

【請求項１８】　時間認証装置のクロック用に計算された較正値は前記装置のメモリ内に記憶される、請求項１７に記載の較正方法。

【請求項１９】　オンチップクロックは、

第１のクロック読み取り以降の振動数をカウントするス

テップと、
調整値を得るために前記振動数を較正値で除算するステップと、
前記調整値を前記第１のクロック読み取りに付加するステップとを用いて、較正値が計算された後に現在時刻を表示する、請求項１７に記載の較正方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、個人用日時認証装置に関し、より特定的には、デジタル署名に付随して日時を認証する装置に関する。
【０００２】
【従来の技術】デジタル署名の出現以来、より多くの取引が電子的に行われる可能性が生じている。デジタル署名を用いることにより、署名操作を行う当事者がその行為を行う権限を適切に有することを、誰からも否認されないように確定することができる。
【０００３】「履歴的」意義を有するデジタル署名には、電子契約に関するものなどがあり、ますます一般的になりつつある。そのような電子契約の場合、特定のデジタル署名がいつなされたか（例えば、公開可能な鍵の取り消し以前か以後か）の証明が可能であることが重要であろう。多くの電子文書、例えば契約書、議事録などとともに、履歴的に重要な署名は保管された記録の一部となっている。そのような署名が正確にいつなされたかを確認できなければ、数カ月前または数年前になされたであろう署名に対して将来において認証を行う場合に、ある時点における公開鍵の取消につき疑念が生じることになるであろう。
【０００４】従って、デジタル署名の日時を確実に知ることが、特に電子的に保存された日記、発明者の科学実験記録、議事録、電子入札または電子契約などのような場合に役立つ。また、第三者に対して、署名時刻および署名主を説得力をもって示す場合にも役立つ。
【０００５】この問題を解決するための１つの方法は、履歴的重要性を有する可能性のあるすべての署名を、例えば本件に援用されている米国特許５，００１，７５２および５，１６３，６４３において説明されているような本出願人の日時認証機構を用いて、「認証」することである。これらの特許は、そのような認証を行うための効果的な方法を述べており、当該認証は、信頼性のある時計を包含した保証装置を用いて行われ、当該装置は、重要なデジタル署名に対し、認証時刻を信頼性のある時間源から取り出して連署する。
【０００６】
【発明が解決しようとする課題】既知のデジタル認証を効果的に用いるには、誰かが事前に署名が履歴的重要性を将来有することを認識し、かつデジタル署名に時刻認証を実施することを思い出す必要がある。また、ユーザは、署名されたもの（またはその寄せ集め）を時刻認証

装置を通して送らなければならない。従って、ユーザは、デジタル署名作成後すぐに信頼性のある時刻認証機構をアクセスしなければならない。
【０００７】実際的に言って、既知のデジタル署名装置は、デジタル署名がなされた時点では用いることができないであろう。署名者は、適時に自分の署名を認証させるのを忘れてしまうかもしれない。このようなことは、デジタル署名をラップトップコンピュータのような携帯型装置で行う場合に、ユーザはたいてい自分の通常の仕事場を離れているので、特に発生しがちである。ものによっては、認証されたタイムスタンプが重要かどうかが署名時点では明確でない場合もある。
【０００８】そこで、本発明は、上記のような従来の方法または装置が有する種々の欠点を解消することを目的とする。
【０００９】
【課題を解決するための手段、作用および発明の効果】本発明は、効果的に、デジタル時刻認証をデジタル署名操作と組み合わせ、タイムスタンプがいつでも自動的に確実に生じるようにしている。ユーザは、タイムスタンプが必要かどうかに関して、いかなる追加の意思決定をする必要がない。別個のタイムスタンプ認証装置の必要性をなくすことによって、ユーザは、時間，経費および労力を節約できる。
【００１０】本発明は、例えばスマートカード，スマートディスク，ＭＣＩＡ装置のようなトークン装置内に設けられ、別個のタイムスタンプ認証装置よりも利用しやすく、ラップトップコンピュータのような携帯型装置と共に用いることも容易である。ここで説明する方法および装置は、効果的に、信頼性のあるタイムスタンプをユーザのデジタル署名操作に自動的に組み込ませることを許容し、ユーザに対して追加のステップを要求しない。本出願人のスマートカード型またはトークン型の媒体は、ユーザのパーソナルコンピュータ（ＰＣ）と共にユーザ宅において、またはラップトップコンピュータのような携帯型装置と共に自宅から離れた場所においてデジタル署名の一部としてタイムスタンプ認証を同時に行うために用いることができる。タイムスタンプ認証をユーザのデジタル署名の一部として同時に得ることによって、いかなる認証者でも当該署名がユーザによってなされたことを証明することができるだけでなく、署名がいつなされたかを証明することもできる。
【００１１】本発明は、それによって信頼性のあるタイムスタンプがユーザ署名に組み込まれ、またはユーザ署名に関連付けられるような種々の代替実施例または実施の態様を考慮している。デジタル証書は、通常、個人鍵／公開鍵に関連した主体の識別および属性を証明するためにデジタル署名を伴う。本発明の実施例に従えば、製造工場は、本発明の個人用日付／認証装置に関連する公開鍵を証明する。また、同じ鍵が、トークン装置の所有

者／オペレータに属する旨を証明することもできる。代わりに、本装置は、ユーザの識別を別個に証明する第２の鍵を含むこともできる。また、証書が装置の外部（例えば認証装置を駆動するコンピュータと関連する記憶装置内）または内部において保存され、所望する場合には署名操作の一部として出力できるようにすることが考慮されている。

【００１２】本発明は、効果的に、すべてのデジタル署名に信頼性のある方法でタイムスタンプを押すことを許容するので、ユーザは、文書がタイムスタンプを必要とするほど重要かどうかを判断する必要がない。本発明に従った認証装置によって作成されたすべての署名は、時刻が正確に刻印されるので、たとえユーザのスマートカードが紛失したり盗難に遭ったり、またはユーザの有する権限が結果的に取消されたりしても、ユーザであることの有効性を自動的に判断することが比較的簡単に行えるようになる。将来のいかなる時点においても、信頼性のあるタイムスタンプを伴ったデジタル署名がいつ行われたかを、容易に決定することができる。

【００１３】

【実施例】本発明の特徴と利点は、以下の図面とともに以下の発明の詳細な説明を考慮にいれることで、明確となるであろう。

【００１４】図１は、本発明の一実施例に従った日時認証装置のブロック図である。装置は、好ましくは「スマートカード」のようなトークン装置１内に設けられる。代わりに、認証装置１は、従来のスマートカードよりも厚みのある、少なくとも数メガバイトの記憶容量を一般的に含むＭＣＩＡカード上に設けられてもよい。媒体１の代わりに、「スマート」ディスケットまたはユーザが携帯または着用可能である実質的にいかなる種類の個人用トークン装置でもよい。もし着用されるアイテム内に設けられた場合、トークン装置は、ユーザの体から脱落したことを感知すると作動しなくなるような機密保護特性を含んでもよい。再起動には、パスワードの入力を要してもよい。そのようなトークン装置を、ユーザが着用した腕時計，指輪，その他宝石または伝統的に私物とされるアイテム（カフスボタン，ネクタイピン，イヤリングなど）にはめ込まれた集積回路内に設けるようにしてもよい。

【００１５】携帯型認証装置１は入力／出力（入出力）ポート２を含み、入出力ポートは、集積回路、好ましくは単一のチップ３に結合している。入出力ポート２は、ＰＣまたはラップトップコンピュータ等に結合される従来型のスマートカード読取装置（図示せず）と結合されてもよい。

【００１６】変更防止秘密個人鍵記憶装置６はチップ３上に設けられる。装置１を変更しようとすると、例えば処理装置４を起動して、秘密鍵を上書きするようにしてもよい。秘密個人鍵記憶装置６は、例えば機密性を有するＲＡＭまたは一度書きメモリであってもよい。秘密個人鍵記憶装置６は、少なくとも、スマートカード１の管理者（または所有者）であるユーザと関連する個人鍵を記憶する。

【００１７】本発明の一実施例に従えば、同じユーザの個人鍵がデジタル時刻認証機能に関連づけられてもよい。代わりに、別の個人鍵を認証機能のために用いてもよい。

【００１８】個人鍵記憶装置６は処理装置４に結合しており、処理装置４は、同様に、処理装置４が実行するプログラムを記憶する固定メモリ８に結合している。処理装置４は、市販の種々のマイクロプロセッサのうちのいずれの一つでもよい。処理装置４は、例えばモトローラ６８０５でもよい。価格やデジタル署名操作を行うために用いるアルゴリズムの実行に必要とされる処理能力といった、当業者に知られている実務上の考慮によっては、特定の処理装置を選ぶべきである。本発明では、ＲＳＡアルゴリズムまたはＤＳＳ（デジタル署名規格）が好ましく、ＲＳＡアルゴリズムについては、リヴェスト等の米国特許４，４０５，８２９において説明されている。しかしながら、モトローラ６８０５とほぼ同様の計算能力を有する処理装置が有用かまたはそれで十分である場合には、ＲＳＡまたはＤＳＳ以外のアルゴリズムを用いることができることも考慮されている。

【００１９】少なくとも１つのクロック１２がカード１上に設けられる。この好ましい実施例において、第２のクロック１４およびランダム値発生器１０も処理装置４に結合している。クロック１４は、実際のクロック値がクロック１２および１４から発生した値の平均とみなされるように、時刻認証装置１の精度を高めるために用いられる。２つのクロックは、相互にチェックし合ってエラーとならないよう確認するために用いることができる。

【００２０】ランダム値発生器１０は、例えば、ダイオードを主体とする周知のノイズ発生装置でもよい。関連の物理的な装置が有する固有のランダム性を利用して、処理装置４がデジタル署名過程において用いる値のランダム性を最大化するような、他のランダム値発生器を用いてもよい。代わりに、ランダム値発生器１０は、周知のソフトウエア技術によって疑似乱数を発生するための固定メモリ８内に記憶された命令に置換されてもよい。集積回路チップ３上に設けられた上述の各構成部分は、適切な寿命の長いバッテリ１６によって電力供給されるが、実施例によっては、ある構成部分には、作動中以外は電力供給されない方が有利な場合もある。

【００２１】本発明の個人用日時認証装置は、好ましくは各々の署名に時刻認証を提供するために用いられるが、所望する場合には、時刻認証を必ずしも提供する必要はない。さらに、処理装置４は、当業者に周知の一般目的の「スマート」カードに関連する処理を実施するよ

うプログラムされていてもよい。

【００２２】次に図２に移って、製造業者が個人用認証装置の初期設定を行う方法を説明する。従来の技術を用いて本装置を組み立て（２０）、その後に処理装置４によって実行されるべきソフトウエアがプログラムＲＯＭ８に格納される（２２）。その後、初期設定操作（２３）が開始する。

【００２３】ブロック２４に示すように、個人／公開鍵の対が作成され、記憶される。この操作は、バッテリ１６が認証装置１に装着された後に生じる。好ましくは、装置１自身が、機密性を有する認証装置環境の範囲外に個人鍵が存在することがないように、装置独自の個人鍵を生成する。しかしながら、個人鍵を外部で生成して装置１内に格納することも可能であるが、機密保護上の理由から内部生成の方が好ましい。好ましくは、個人／公開鍵の対が上記米国特許４，４０５，８２９で説明されているＲＳＡアルゴリズムを用いて作成される。しかしながら、その他のアルゴリズムを個人／公開鍵の対を作成するために用いてもよい。

【００２４】公開鍵は、ある時点で入出力ポート２を通って出力されるが、最初に鍵を格納する過程では出力は不要である。好ましくは、公開鍵は、認証装置クロック１２および１４の両方がセットされるまでは出力されない。この予防策を講じる場合には、装置１は、いかなるデジタル署名もなすことが可能となる以前に初期設定が完全に行われていなければならない。ブロック２６に示す初期設定過程の一部として、認証装置１は高精度の正確さを有するマスタクロックから現在の日時を受け取る。本発明の好ましい実施例に従えば、クロック１２および１４は、エラーおよび故意に変更しようとする可能性を減少させるために、どちらも装置１内に設けられる。製造業者のマスタクロックは、世界中で認識されているグリニッジ標準時に従ってセットされることが考慮されている。製造業者のマスタクロックの出力は、入出力ポート２を通って処理装置４に入力され、その後でクロック１２および１４に入力されている。処理装置４がクロック１２および１４の出力時間の差を監視しているので、２つのクロックを用いることによって、処理装置はクロック１２が適切に機能しているかどうかを判断することができる。

【００２５】ステップ２８で示すように、この好ましい実施例においては、１日または１週間のような一定期間後に、認証装置１は同じマスタクロック（または他の正確なクロック）と再同期され、このハードウエアに特有の「クロックドリフト」が決定される。この調整要素は、後に装置の固定メモリに保持される。マスタクロックから第１クロック読み取りを行い、この第１クロック読み取りを記憶し、マスタクロックから第２クロック読み取りを行い、この第２クロック読み取りを記憶し、両方のマスタクロック読み取り間の振動数をカウントすることにより、較正されたクロック読み取りを決定することができる。その後、実際の振動周波数は、第２と第１のマスタクロック読み取りの差で除算した振動カウントを用いて単位時間当たりの振動を計算し、この計算後の振動周波数を記憶し、オンチップクロック装置の出力を計算後の振動周波数に従って調整することによって計算することができる。較正後の現在時刻は、以下のステップにより計算することができる。第１クロック読み取り（ベンチマーク時刻）以降の振動数をカウントし、較正値によってこの値を除算し、その結果を前記第１クロック読み取りに加算する。振動周期と比較してマスタクロック読み取り誤差が大きいと思われる場合には、クロック精度は、２つのマスタクロック読み取りの差で除算されるマスタクロック読み取りの不正確さの２倍を超えない程度の正確さとなる。従って、１週間後のマスタクロックの読み取り誤差が０．２５秒であれば、較正後の精度は１００万分の１秒以上となる。このようにして、製造差の結果として存在する個々の偏差を補償することができる。

【００２６】多くのデジタルクロックが気温によって僅かに変化することが知られているので、もし２つのクロックを用いるならば、異なる方法、できれば異なる材料または構造でクロックを組み立てることが可能であり、気温の変化はクロックに対してそれぞれ知られ理解される異なる影響（例えば、異なるドリフト係数）を与えるようになる。そのようなドリフトは僅かだが、気温の変化による進行中のクロックドリフトを検出して明らかにするための第２番順位の補正として用いることができる。一旦、両クロックを較正すれば、例えば、既知の管理気温では、いかなる相互の偏差も、たとえ僅かであっても、実際には、気温の計測および内部補正を行うために用いることができる。当然のことながら、これと同様の方法は、外部の影響に基づく既知の方法でクロックがドリフトされるような、いかなるデジタルクロック装置内においても用いることができる。

【００２７】図２のステップ３０に示すように、この時点で装置の初期設定が完了するようになっている。プログラムは、一旦格納すると、すなわち秘密鍵が利用可能になるや否や、すべてのメモリ（秘密鍵記憶装置を含む）が消去されない限り他のデータまたはプログラムが格納できないように設計されている。クロックの格納過程は一度だけ生じるようになっている。

【００２８】電力が消失すると、クロックが無効になってしまうので、間違った時刻読み取りを行わないように装置が作動しなくなるように設計することも考慮されている。

【００２９】ステップ３２で示すように、製造業者は、認証装置に機密に記憶された個人鍵に関連する公開鍵が信頼性のある認証装置に属することを証明する。製造工場の証明がなされる前に、正確性および耐久性につき装

置をさらにテストすることが望ましいであろう。製造業者は、作成された公開鍵はこの特定のユーザの認証装置とともに用いられることが許可された旨を示す証書を作成する。この製造業者の証書は、以後、カード１と関連づけられる。

【００３０】好ましい本実施例によれば、処理装置４により実行されるプログラムがＲＯＭ８に格納された後に、プログラムが実行され、ステップ２４から３２を行うか、または（例えば、ステップ２６および２８おいて要求されているように）製造業者のマスタクロックとの関連を少なくとも促進することによってこれらのステップの実行を補助する。

【００３１】図１の認証装置は、代替し得る様々な実施例および実施態様に従って実施されるように設計されている。第１の実施例は、単一の個人鍵を用いる。この実施例では、単一のデジタル署名結果および単一の証書が存在する。証書は、特定のユーザが信頼性のある認証装置内の個人鍵で操作している旨を証明する。この実施例では、証明者は、ユーザの証書において、ユーザの個人鍵は機密性を有する装置内で信頼性のあるクロックとともに実施されていることを明確に示す。これは、もし証明者がユーザに対してユーザの個人鍵が信頼性のあるクロックと共に機密性を有する装置内で作動することを証明するだけだと（明示的にであろうと黙示的であろうと）知られていたとしても、間接的に達成され得るであろう。

【００３２】公開鍵が機密性を有する時刻装置内の個人鍵と整合することを証明権限者が確認し得るような方法はいくつかある。例えば、装置製造業者が公開鍵と信頼性のある装置とを関連づけて発行する証書を用いてもよい。実際には、ユーザの証明者は、単一の証書のみが必要となるように、装置がユーザの個人鍵を含むことおよび装置が信頼性のある時間を提供することを保証する。この実施例の利点は、各公開鍵は１つの即時証書しか伴わないという点にある。これに対し、他の実施例は、２つの即時証書を必要とし、１つは個人に対し拘束性を有し、識別を行う証明権限者による証書であり、もう１つは機密性を有するクロック装置である旨を示す製造業者発行の証書である。

【００３３】この第１の実施例を用いると、公開鍵がユーザと関連することを単に確認するために通常取られるステップ以外に、証明者またはユーザによるさらにいくつかのステップが必要とされる。追加のステップでは、ユーザの公開鍵が確かに信頼性のある日時認証装置とも関連があることを確認する。

【００３４】ユーザを証明するために、まず効力確認ステップが実行され、そこでは製造装置が提供する効力確認証書が、当該公開鍵は適切に認証装置と関連する旨を示す。ユーザの公開鍵が認証装置と適切に関連していることは、当該鍵が認証装置と適切に関連していることを

確認するための予め定められた応答を得ることを期待して呼び掛けを発することにより確認することができる。実際の装置が期待通りの署名（期待された公開鍵と共に認証されている）を作成したことを証明者が確信するように、認証装置は、証明者の面前で証明者によって提供されたランダム呼び掛けデータに対し動作することができる。また、証明者は、装置が作成した日時が正しいかどうかも確認する。

【００３５】認証の後、証明者は、装置の公開鍵のための証書を作成し、当該証書は、指定のユーザが信頼性のある認証装置を通して操作する旨を公開鍵が反映していることを示している。そのような表示は、証書において明示的にまたは黙示的に示され、黙示的な場合は、例えば信頼性のある認証装置からユーザが公開鍵を操作したことを単に証明者が証明することが知られている場合である。

【００３６】本発明は、２つの証書が同一の公開鍵用に作成されるという点を除き、第１の実施例に類似した第２の実施例に従って操作されてもよい。１つめの証書は「製造工場」から生じたもので、関連する個人鍵が信頼性のある認証装置内に存在することを確認し、２つめの証書は証明権限者から生じたもので、ユーザと公開鍵との関連性を確認する。

【００３７】第２の実施例では、第１の実施例と同様に、装置はユーザと関連する単一の個人鍵を含む。この個人鍵は、装置製造業者によって、機密性を有する認証装置環境内で作動することが証明されている。また個人鍵は、識別権限者が認証装置の個人鍵とそれを操作する個人との関連性を確認することによって証明される。

【００３８】装置を操作することによって、署名されるべきデータ（電子文書）またはその派生物（例えば寄せ集め）を含む構成と、内部の信頼性のあるクロックから装置によって決定された現在時刻とが作成される。個人鍵が、この全体構造（またはその寄せ集め）にデジタル署名を行うために用いられる。

【００３９】引き続いて、この署名は、装置１内に記憶された秘密個人鍵と関連する公開鍵を有するいかなる主体によっても認証されうる。さらに、製造業者およびユーザの鍵に関連する２つの証書を保持することにより、認証を行う主体は署名鍵が特定のユーザと関連し、また与えられたタイムスタンプが信頼できるものであることを決定することができる。

【００４０】認証者が署名およびタイムスタンプが有効であることを確認するために実行するステップには、１）署名値、関連する公開鍵および挿入されるタイムスタンプに必要とされる様式に基づいて、署名が正しく形成されているのを保証するステップと、２）ユーザの証書情報は、有効であり、かつ認証者が信頼し（それによってユーザの身元を認証する）元証書をたどるのを保証するステップと、３）認証装置の製造業者によって提供

される証書情報には、当該装置は信頼性のあるクロック値を署名に組み込んでいる旨と、認証者は製造業者が信頼性のあるタイムクロックを組み込んだ装置を証明するのを信頼している旨とが記載されるのを保証するステップとが含まれる。

【００４１】図３は、本発明の上述の第１および第２の実施例に従った操作を例示したフロー／ブロック図である。図３に示すように、署名されるべきデジタル値／文書４０は、入力ポート４１経由でスマートカードインタフェイス装置（図示せず）を通ってカード１に入力される。値４０は処理装置４に入力され、そこで、ステップ４２に示すように、値は一時的に記憶される。

【００４２】処理装置４は、その後、現在の日時をボード上の信頼性のあるクロック（１２，１４）から抽出し、このデータをブロック４４で示すように記憶する。署名されるべきデジタル値／文書４０（またはその派生物、例えば寄せ集め）は、ブロック４８で示すように、不明確でない方法で現在の日時と組み合わされる。ステップ５０で、結み合わせ値は、既知の公開鍵暗号方法に従って、記憶装置６に記憶された秘密個人鍵で署名される。所望すれば、デジタル署名操作を行う以前に、処理装置４がユーザの個人識別暗証（ＰＩＮ）をまず確認するようプログラムしておいてもよい。

【００４３】第１および第２の実施例に従えば、認証装置１は個人鍵記憶装置６に記憶された単一の個人鍵を用いる。署名済の値の結果は、ステップ５４で、図１に示す入出力ポート２の一部である出力ポート５６に送信される。出力ポート５６に入力されるデジタル値は、信頼性のあるクロック１２および１４から抽出された日時印を含むデジタル署名である。

【００４４】スマートカードインタフェイス装置（図示せず）を通って、出力ポート５６からの出力値は、好ましくは、パーソナルコンピュータまたはラップトップコンピュータのような外部処理装置（５８）に入力される。ステップ６２および６１に示すように、必要とされるようないかなる証書もプルーフパケット６０に入力される。プルーフパケット６０は、個人用署名認証装置のオペレータ／所有者に関する公開鍵の識別を証明済みであり、公開鍵が信頼性のある日付で認証された個人の署名を形成する認証装置に組み込まれていることを証明する。

【００４５】このような証書、出力ポート５６からの出力値および元のデジタル文書は、本発明のこれらの実施例によって作成された署名プルーフパケット６０を形成する。証書を元にしたデータ、認証装置１の出力およびデジタル文書４０は、既知の公開鍵暗号規格に従って、デジタル署名に付随する文書を付加するために組み合わされる。プルーフパケット６０はユーザのコンピュータシステム（５８）に記憶され、様々な方法で索引を付けることができる。例えば、署名された値は発明者の日誌

に現在の日付の見出しを示し、発明者の日誌と関連したファイルとして索引を付けてもよい。認証装置１が充分な記憶容量を有する場合には、カード内に設けられた処理装置４を用いてプルーフパケットを作成し、関連するメモリ内にパケットを記憶することも可能であろう。しかしながら、プルーフパケット６０の作成操作では、高度な安全性は要求されないので、このような操作は、カード１外のユーザのコンピュータで行われてもよい。

【００４６】本発明の第３および第４の実施例に従えば、個人鍵記憶装置は２つの個人鍵を記憶し、２つの異なる署名を作成する。第１の個人鍵は認証装置に関連する個人鍵であり、第２の個人鍵は特定のユーザに関連する個人鍵である。認証装置の個人鍵を、上述のように（一般的に装置自身が）工場で生成するのは、公開鍵が機密性を有するクロック装置に属していることを証明して、クロックがまず較正されたときである。ユーザの個人鍵も、好ましくは装置自身が生成し、認証装置を操作または所有するユーザに属する旨が証明される。

【００４７】この実施例では、操作は、２つのデジタル署名を作成する装置から構成され、一方はユーザの個人鍵で署名を作成し、他方はタイムスタンプに関連する装置固有の個人鍵で署名を作成する。署名作成の時刻および順序にはいくつかの方法がありうるが、署名されるデータの寄せ集めは信頼性のあるクロックの現在値と組み合わされ、この組み合わせ結果がユーザの個人鍵で署名されるのが好ましい。さらに、この署名は装置の公開鍵で署名される。代わりに他の署名シーケンスを用いてもよい。例えば、対象物がユーザの個人鍵で署名され、さらにその結果が装置の認証鍵で署名されてもよい。この場合、最終結果は、ユーザの署名にタイムスタンプを押すために別個の認証装置を用いた結果と類似するように見えるかもしれない。この方法は、より従来の認証技術と適合し易いであろう。認証は、両署名（ユーザの公開鍵および認証者の公開鍵）を認証し、効力および信頼性を確認するため各証書をチェックすることによって、この第３の実施例に関連する操作が行われたときに実行される。

【００４８】第３の実施例は、第１の実施例と類似するが、初期設定の過程が異なる。図２に戻って、第３の実施例に従って操作すると、第２の個人署名鍵が作成され、装置の機密保護メモリ６に記憶されるような、さらなる初期設定のステップを行わなければならない。従って、認証装置は、メモリ６内に記憶された２つの個人署名鍵を含み、第１の鍵は認証装置の製造工程で（理想的には認証装置自身により）生成される。第２の鍵は後に生成され、ユーザと関連づけられてもよい。実際には、いくつかの異なるユーザ鍵が生成され、装置に保持されうる。本出願によれば、複数の鍵が並行または同時に存在することを許容するのが望ましい。

【００４９】本発明の第４の実施例によれば、認証装置

は、好ましくは、スマートディスケット内に設けられ、このスマートディスケットは本発明で援用されている公開ドイツ特許出願Ｐ４１１２０２３．９に従って作成される。装置は、財布の大きさくらいのスマートカードとＰＣのディスク読取装置との間でインタフェイスとして動作する。この実施例では、認証装置は、単一の要求の一部としての時刻認証を達成するために、スマートカード（または他の従来のデジタル署名装置）と協働する、機密性を有するインタフェイスとして動作する。

【００５０】この第４の実施例の認証装置は、ユーザの個人鍵を含んでおらず、署名されるデータを提供するコンピュータ（またはその他の手段）にスマートカード装置を結合するインタフェイス（または「読取装置」）に過ぎない。装置は、時刻認証装置をユーザの個人鍵操作を実行するスマートカード装置に結合させるように動作する（この場合、スマートカードは信頼性のあるクロックを有しない）。この場合、時刻認証装置はスマートカード読取装置と結合しているとみなすことができる。

【００５１】この実施例では、装置は、署名されるデータおよび刻印される時刻が認証装置に提供されるように動作する。装置は、ユーザの個人カードを操作するユーザのスマートカードをインタフェイスし、署名結果を戻す。スマートカードから装置へ戻される署名結果（または署名から派生するある値）は、装置によって装置自身の個人（認証）鍵でデジタル的に署名される。組み合わされた署名結果はその後装置の発呼者に戻される。この場合、結果は、上述の実施例で作成された（２つの署名および２つの証書を用いた）結果と類似するように見える。このインタフェイスに基づく実施例に従えば、時刻認証装置は、時刻が刻印されたユーザデジタル署名の有効な「同時」実行を許容するスマートカード読取装置として動作する。この実施例は、実質的には、スマートカード読取装置であって、ホストＰＣまたはその他のハードウエア装置に対して時刻が認証されたデジタル署名を作成する時刻認証装置を含む。

【００５２】第３の実施例に従えば、図３に示す操作は、ブロック４２の操作が署名されるべき対象物のユーザの個人鍵によるデジタル署名を実際に作成するように、変更されなければならない。従って、ボックス４２からの出力値は、「認証されるべき値」４２となる。

【００５３】同様に、図２の初期設定過程は、排他的にユーザを示す第２の公開鍵／個人鍵の対が作成されることを示すように、拡張されなければならない。しかしながら、これは装置が工場から出荷された後でも作成することができ、また、（製造業者が証明した後は変更が効かない認証鍵とは異なり）ユーザの要求で作成することもできる。実際、いくつかの異なるユーザ個人鍵も存在しうる。

【００５４】第４の実施例に従えば、図３に示す操作は、ブロック４２の操作がユーザの個人鍵トークンとともに適切なポートを通って実際に通信を生じさせるように、変更されなければならない。この実施例の場合、ボックスに示す処理は個人用認証装置（１）内では発生しないが、ボックス４２の出力は、（第３の実施例のように）署名されるべき対象物のユーザ個人鍵によるデジタル署名である。よって、ボックス４２からの出力値は、「認証されるべき値」４２となる。

【００５５】組み合わされた結果値は、その後、（製造工場で作成され、証明された）認証個人鍵で署名される。署名後の組み合わされた結果値は、出力ポート５６へ出力される。ステップ５８では、（ユーザおよび装置の）両公開鍵に必要な証書が最後のプルーフパケット結果に組み込まれる。

【００５６】さらに代替可能な実施例では、信頼性のあるスマートカードクロック装置は、スマートカード自体の中に信頼性のあるクロックを設けることなく、個人用スマートカード型装置が信頼性のある日時認証を単一のデジタル署名結果に組み込めるように実施される。このことは、より制限された（クロックのない装置）が、（第３の実施例にあるように、信頼性のあるタイムスタンプを単一の個人デジタル署名に組み入れたのと）同一の署名結果を提供することを許容するが、スマートカード型装置のボード上には、信頼性のあるクロックは存在しない。この目的を達成するために、スマートカードは、前述のドイツ公開特許書類で説明されているスマートディスケットを用いた上述の実施例とは異なるプロトコルを用いた日時認証機構に結合される。

【００５７】信頼性のあるクロック署名は、信頼性のある認証装置と共に用いる場合のみ可能であるが、これは、他の場合でも容認できる。信頼性のあるクロックデジタル認証機構は、スマートカードおよび読取装置の協働作用が上述の代替実施例によって作成されたのと類似または同一の日時認証されたデジタル署名を作成するように、スマートカード読取装置に組み込むことができる。

【００５８】図４はこの代替実施例に従った操作を示し、この実施例が図３に示される方法にどのように組み込まれるかを示している。図４のステップ４８０および図３のステップ４８は同一の操作を示している。その後、図３に関連する上述したような操作がさらに続く。

【００５９】図４に示すように、スマートカードには、デジタル署名および日時認証が行われるべき値４１０が与えられる。ブロック４２０に従って、スマートカードは特有値を作成し、この値を信頼性のある日時認証装置に与える。これは、侵害者が通信内に失効した日時値を何とか取り込もう（「再生しよう」）と試みるのを防止するために設計されている。この特有値は、選択的に、オンボードランダム値発生器によって作成されるか、または署名される値に基づく。

【００６０】ステップ４３０に従って、特有値はスマー

トカード読取装置と結合されているかまたはそれに組み込まれている信頼性のある日時認証機構によって提供される。ステップ４４０に従って、信頼性のある日時装置は、現在の時間と関連して署名することによって、与えられた特有値を認証し、スマートカードに戻す。信頼性のある日時認証装置は、証書（または証書階層）も戻すのが望ましい。この証書は、通常、認証機構の製造業者によって作成されるが、このタイムスタンプが正確で信頼性のあることをスマートカードに対して証明する役割を果たす。

【００６１】ブロック４５０に従って、この署名済の値を受信すると、スマートカードは、認証結果が上述のステップ４２０で提供された特有値について行われたことを証明する。さらにスマートカードは、認証値の与えられた証書は正確に認証署名を記載していること、および証書は署名が実際に信頼性のある認証装置によって作成されたことをスマートカードが決定するのに充分な情報を含んでいることを証明する。最終的には、この情報は、製造時にスマートカードに格納された元情報に基づいて証明される。そのような元情報は、例えば認証製造業者による元証書またはその公開鍵（またはその寄せ集め）を含んでいてもよい。認証装置によって与えられた証書が、スマートカード内に記憶された情報（例えば、認証機構装置内の公開鍵，認証装置の製造業者の公開鍵またはそれらの寄せ集め）に従って認められた権限者によって署名されたとすると、スマートカードは、現在の信頼性のあるクロック値を有すると推定される。認証の一部として、スマートカードは、認証値がステップ４２０で最初に与えられた特有値から抽出されたものであることを保証する。

【００６２】ステップ４６０に従って、スマートカードは、その後、信頼性のある日時認証装置を内部に備えているのと同程度の信頼性を有効に有する認証装置によって与えられた日時を用いる。従って、信頼性のある日時を、ユーザの公開鍵を用いて行われる署名操作に組み込むことができる。スマートカードは他の場合（または信頼性のある日時認証に結合していない読取装置）でも用いることができるが、作成された署名は、日時認証とは結合されない。その後、図３に示す実施例に従って署名が作成され、図３に示されたステップ４８に従って操作が進む。

【００６３】さらに代わりうる実施例として、スマートカード型装置は、まずユーザの個人鍵を適用し、次に、ユーザの署名およびタイムスタンプ認証された署名がそれぞれ個別の識別子を内部に有する、結合されたスマートカード型インタフェイス／タイムスタンプ認証装置に対し、その署名をデータとして提供する。この場合、時間／認証装置およびスマートカード読取装置（インタフェイス）の結合は、ユーザの署名に対する簡便な時間認証を提供し、その形式は、出願人の米国特許５，０１

１，７５２または５，１６３，６４３に概説されるような日時認証の他の使用法と同一である。種々の好ましい実施例がタイムスタンプを常に提供するが、タイムスタンプが条件付きで提供されるように実行してもよいことが考慮されている。

【００６４】図５は、典型的なプルーフセット５００がどのように認証されるかを示すフロー図である。認証操作には特別な機密保護措置を行う必要がない。署名された文書を受信する受信者が、上述のように署名を認証する。

【００６５】受信者が受信するのは、対象の値１０を含むプルーフセット５００、すなわち本発明の認証装置によって作成された署名を有するデジタル文書であって、署名済の対象の値の寄せ集め５０８，信頼性のある認証装置によって作成されたとされる日時５０４（後続の認証ステップにおいて証明される）およびユーザが操作する装置内にある個人鍵を上記情報に当てはめることによって作成される印５０６を含む。さらに、プルーフセットは、証書６２および６４を含み、これらの証書は、（装置内に記憶された個人鍵に対応する）公開鍵がユーザに属し、信頼性のある日時認証と関連して操作されることを証明する。

【００６６】署名を認証する主体は、以下のステップを実行する。署名操作は、署名されたデータを正しく反映していることおよび「表明された」日時とともに正しく構成されていることを示すことが認証される。値１０の寄せ集め（出力５０８）、日付５０４および印５０６は５１０において署名操作を認証するために入力される。印が日付５０４（５１０で決定される）を正しく反映していれば、無効な署名が検出されたかどうかがブロック５２０において決定される。もし無効な署名が検出されると、「無効な署名」というメッセージ５２５が受信者に伝達される。もし印５０６がデータを正しく反映していれば、ブロック５３０に処理は継続する。ブロック５３０に示すように、ユーザの証書は、署名者の識別が署名者の公開鍵と適切に関連していることを確認するためにチェックされる。さらに本発明は、所望すればユーザが有する権限を認証することも考慮しており、その方法は、米国特許５，００５，２００で説明されている方法に関連した出願人の拡張デジタル署名に従う。

【００６７】ステップ５４０に従って、利用可能な証書（または他の情報）のどれかを用いて、公開鍵（本発明の第１の実施例に従うユーザのための証書６２と同一であろう）が、証書６４の内容に基づく信頼性のある日時認証装置の予想される種類と関連し、かつそこから操作されることが確認される。詳細な認証ステップは、上述の実施例のどれが用いられるかによって異なるであろうことが理解されるべきである。

【００６８】ステップ５５０に従って、認証鍵が有効で、かつ信頼性のある日時認証装置に属するかどうかを

17

決定するためのチェックが行われる。もし認証鍵が有効でなければ、受信者が認証および日付を信頼できない、旨のメッセージが作成される。代わりに、もし有効な認証鍵が検出されれば、ブロック５７０で示すように、ユーザの識別および認証日時の確認がなされる。

【００６９】個人認証鍵およびユーザの個人鍵を用いて複数の署名が行われる上述の実施例では、認証は図５に関して上述した認証と類似しており、異なる公開鍵によって行われる複数の認証が、複数の署名を認証する際に用いられる点が異なっている。

【００７０】個人識別番号（ＰＩＮ）パスワードが上述の実施例に関して用いられる場合、当該パスワードは、トークン装置へのおよび／またはそこからの情報を署名または送信するために、種々の方法、例えば１）署名要求と共に、２）トークン装置と関連する公開鍵で暗号化されて、３）トークン装置と共通の秘密鍵で暗号化されて、４）暗号化鍵として用いられて、または暗号化鍵を抽出して、トークン装置へ提供される。

【００７１】本発明は、現時点で最も実用的かつ好ましい実施例と思われる事項に関して説明されてきたが、本発明は開示された実施例に限定するものではなく、添付のクレームの精神および範囲内において、種々の修正および同様の構成を含むことを意図していることが理解されるべきである。

18

【図面の簡単な説明】

【図１】図１は、本発明の個人用日時認証装置の一実施例のブロック図である。

【図２】図２は、製造業者が個人用日時認証装置の初期設定を行う場合の方法を説明するフロー図である。

【図３】図３は、認証装置が本発明の第１および第２の実施例に従ってどのように動作するかを示すデータフロー／ロジック図である。

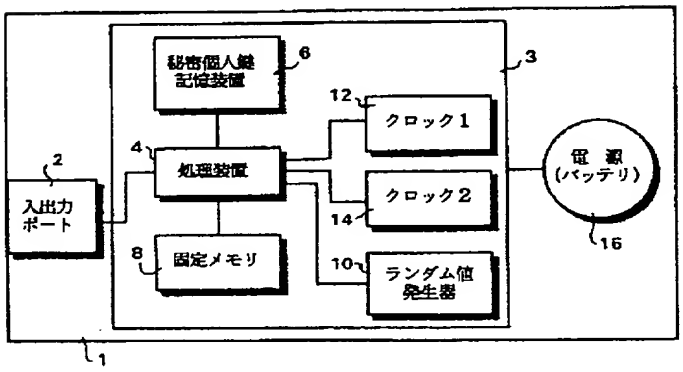
【図４】図４は、個人用日時認証装置がさらなる実施例に従ってどのように動作するかを示すフロー図である。

【図５】図５は、本発明の認証装置によって発生されたプルーフセットがどのように認証されるかを示すフローチャートである。

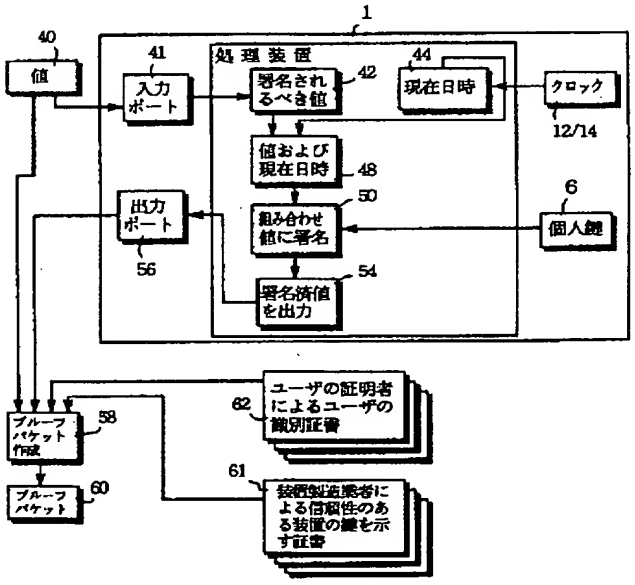
【符号の説明】

１…携帯型認証装置
２…入出力ポート
３…チップ
４…処理装置
６…秘密個人鍵記憶装置
８…固定メモリ
１０…ランダム値発生器
１２，１４…クロック
１６…電源

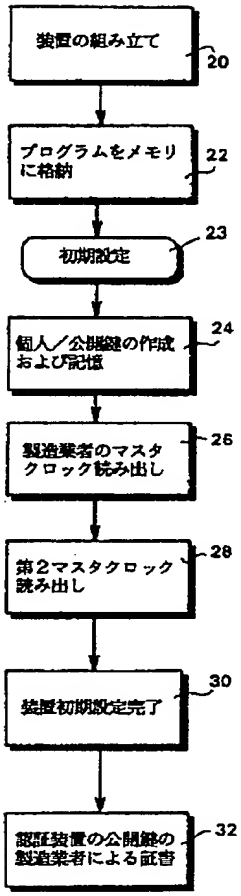
【図１】



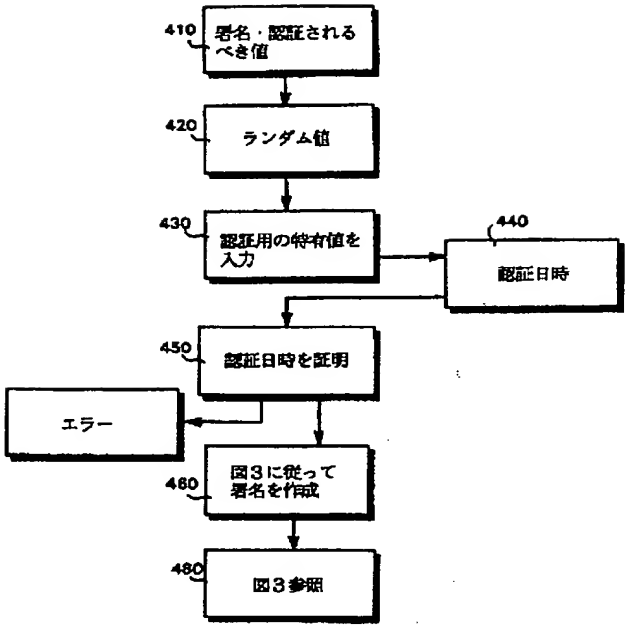
【図３】



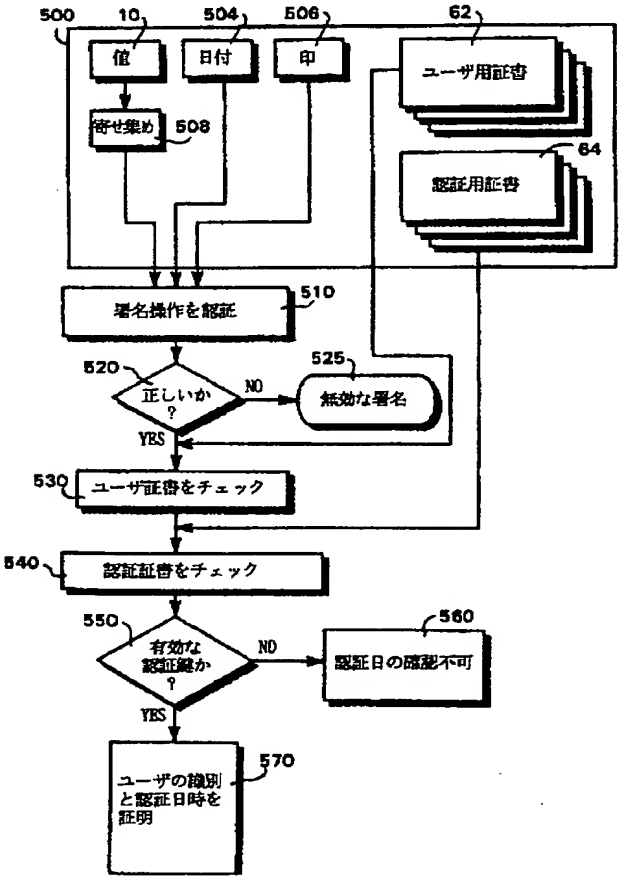
【図２】


装置の組み立て
20
プログラムをメモリに格納
22
初期設定
23
個人／公開鍵の作成および記憶
24
製造業者のマスタクロック読み出し
26
第2マスタクロック読み出し
28
装置初期設定完了
30
認証装置の公開鍵の製造業者による証書
32

【図４】


410
署名・認証されるべき値
420
ランダム値
430
認証用の特有値を入力
440
認証日時
450
認証日時を証明
エラー
460
図３に従って署名を作成
480
図３参照

【図５】


500
10
504
506
62
値
日付
印
ユーザ用証書
寄せ集め
508
64
認証用証書
署名操作を認証
510
520
正しいか？
NO
525
無効な署名
YES
530
ユーザ証書をチェック
540
認証証書をチェック
550
有効な認証鍵か？
NO
560
認証日の確認不可
YES
570
ユーザの識別と認証日時を証明

フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｋ　1/00		Ｚ		